AU/AWC/RWP039/96-04

AIR WAR COLLEGE

AIR UNIVERSITY

THE NEED FOR A USAF INFORMATION WARFARE (IW) STRATEGY FOR MILITARY OPERATIONS OTHER THAN WAR (MOOTW)

by

Bradley L. Butler
Col, USAF

A Research Report Submitted To the Faculty

In Fulfillment Of the Curriculum Requirement

Advisor: Dr. George Stein

Maxwell Air Force Base, Alabama

1 April 1996

24 OCTOBER 1997

POC: AIR WAR COLLEGE.
ADVANCED AIRPOWER STUDIES
MAXWELL AFB, AL 36112

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Page

Abstract

With the end of the Cold War, much has been written recently about the future direction the U.S. should take in an uncertain and rapidly changing world environment. Should America expand endeavors into the world community, or focus more attention and resources on domestic problems? The decision will have far reaching implications for many years to come. Two areas having an impact on the answer to this question but not normally examined together are information warfare and the broad area of military operations short of large-scale conventional combat operations commonly known as military operations other than war (MOOTW) and very recently alluded to as other military operations (OMO).

Revolutionary advances in computers, as well as huge and rapidly expanding computer and communications networks, have created an information explosion with far-reaching political, military, economic and social implications for all mankind. Control of this huge amount of information has become a major issue among numerous competing groups, lending the term "information warfare" a whole new meaning not previously associated with societies in which change occurred at a much slower pace. Control of intangible information assets is increasingly replacing control of tangible assets as a source of real power.

As we enter the Information Age, the end of the Cold War has also created another major series of changes, unleashing many new forms of competition in MOOTW. It is

becoming increasingly obvious to most observers that large-scale conflicts between nation states are being replaced by other forms of conflict and competition. Yet for a number of reasons Air Force doctrine says little on the subject, and even less about the impact the information age in general and information warfare in particular will have on it.

This paper examines both the information warfare environment and MOOTW to determine emerging information warfare technologies that may impact on MOOTW, as well as to determine those types of MOOTW requiring unique information warfare capabilities not currently planned for in large-scale conventional warfighting operations. The limitations of using information warfare in MOOTW are also examined in some detail. The author contends that although emerging Air Force strategy and doctrine on information warfare should attempt to address MOOTW more than it currently does, in general strategy and doctrine will be subject to more constraints than corresponding information warfare strategy and doctrine for mid- to high-intensity conflict.

Chapter 1

Introduction

> *Thus, what is of supreme importance in war is to attack the enemy's strategy; next best is to disrupt his alliances: the next best is to attack his army. The worst policy is to attack cities. Attack cities only when there is no alternative. . . . Thus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations.*[1]
>
> —Sun Tzu, *The Art of War*

The Future Face of War

Much has been written recently regarding the most likely conflicts the U.S. may face in an uncertain, rapidly changing world environment. To a large degree this discussion has been driven by historical events: the rapid onset of the information age, Vietnam, and the end of the Cold War. As the sole remaining superpower, U.S. attention is constantly requested around the world, stretching our resources to the limit. U.S. leadership is under the gun as we try to manage global interests. Should we expand endeavors into the world community, or focus more attention and resources on domestic problems while we have the opportunity? The decision will determine our fate for decades to come.

New technologies are also having a major impact on current thinking. Advances in computers and the establishment of a huge and rapidly expanding global communications network are revolutionary. The full implications associated with the resulting informa-

tion explosion being produced from this area of growth are truly mind-boggling. Suddenly, "there's a new war out there, and it's about who controls the information. It's all about the information."[2]

The downfall of the Soviet Union appears to have momentarily lessened the threat of all-out nuclear confrontation and large-scale conventional war, but the end of the Cold War has also unleashed many new forms of competition in the large conflict grouping we call "military operations other than war." It seems obvious to most observers that the vast majority of problems confronting the U.S. in the future will take place in this arena, yet for a variety of reasons Air Force doctrine says little about this subject, and even less about the impact the information revolution will have on it.

This paper contends that emerging Air Force strategy and doctrine on information warfare should attempt to address military operations other than war, but in general will be subject to more constraints than corresponding information warfare strategy and doctrine for mid- to high-intensity conflict.

Notes

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 77-79.

[2] Cosmo in the movie *Sneakers.*

Chapter 2

The IW Environment

It has belatedly begun to dawn on people that industrial civilization is coming to an end. Its unraveling . . . brings with it the threat of more, not fewer, wars—wars of a new type.[1]

—Alvin and Heidi Toffler, *War and Anti*-War

General

Several factors affect today's IW environment as it relates to national security. To put things in proper perspective, it is useful to begin the discussion with a brief review of recent events that are shaping this environment. Major historical events include, but are not limited to, the transition to the information age, the loss in Vietnam, and the aftermath of the Cold War. Next, it is useful to examine several of the major reasons *why* information wars will be fought. Finally, an overview of the various components of the IW environment is in order. These environmental components include the information infrastructure; the legal, regulatory policy environments; emerging technologies; and adversary capabilities. This chapter briefly examines each of these areas.

Major Historical Events

The Transition to the Information Age

Alvin and Heidi Toffler argue convincingly that a new civilization is beginning to emerge in our lives, one that is radically changing family styles and every aspect of the way we work, manage the economy, and maintain political relationships. Up to this point in history the human race has already undergone two great waves of change, each of which largely replaced earlier cultures or civilizations with ways of life inconceivable to those who came before. The First Wave—the agricultural revolution—took thousands of years to complete. The Second Wave—the industrial revolution—took approximately three hundred years. The Third Wave—the information revolution—will occur even more quickly, probably in only a few short decades. Most of us therefore will feel the full impact of the Third Wave in our own lifetimes—an impact that will cause the greatest social upheaval and creative restructuring of all time.[2]

In the words of the honorable Newt Gingrich, Speaker of the U.S. House of Representatives:

> The Tofflers correctly understand that development and distribution of information has now become the central productivity and power activity of the human race. From world financial markets to the worldwide, twenty-four-hour-a-day distribution of news via CNN to the breakthroughs of the biological revolution and their impact on health and agricultural production—on virtually every front we see the information revolution changing the fabric, pace and substance of our lives.[3]

Winn Schwartau, a computer expert and author, describes in superb detail many of the ways in which we must come to terms with this new Information Age. He contends that the U.S. is already at war, a war that few of us have bothered to notice. The

twentieth century information skirmishes that have occurred thus far are but a prelude to global Information Warfare. He notes that although the Cold War is over, it has been replaced by economic warfare, and the U.S. can expect others to expend considerable efforts aimed at the informational and financial infrastructure upon which our economy depends.[4]

Intense competition is shaping up between three major trading blocks: North America, Europe, and the Asian Pacific Rim. These three huge economic forces account for about one quarter of the earth's population and 80 percent of its GNP. The stakes are enormous.

Our modern society is based on the availability of access to information that will drive a thriving economy upward on its course or propel a weak one into a position of power. With a vast and rapidly expanding network connecting world societies more and more each day, the implications are profound. Information moves almost instantaneously anywhere we choose, is intangible, yet of immense value. Today's information is the equivalent of yesterday's factories, yet it is considerably more vulnerable. Computers and other communications and information systems have suddenly become very attractive first-strike targets; the U.S., which depends heavily on these systems, is very vulnerable.[5] Simply put, the United States is not ready to defend itself or its economic interests against a dedicated information warrior or economic aggressor. From a military perspective, our economic vulnerability is patently unacceptable.[6]

The Loss in Vietnam

It is hard to imagine a conflict involving more disparity in tactics and technology that that between the U.S. forces in Vietnam and their Vietcong and North Vietnamese

opponents. Tiny pajama-suited men carrying AK-47 rifles, crude rockets, and homemade explosives were paired off against the might of American gunships, artillery, century-series fighters and B-52 bombers. Although we always prevailed on the battlefield, the war dragged on for over eight years—and we lost. The price was high: 58,000 dead, and a divided and disillusioned nation.

Even after the war, we just couldn't understand how we could have lost. The remark made by Col Harry G. Summers to his North Vietnamese counterpart is typical of the U.S. mindset. In a final meeting between the two belligerents following hostilities, Col Summers said, "You know you never defeated us on the battlefield," to which the North Vietnamese colonel replied, "That may be so, but it is also irrelevant."[7]

The overwhelming urge to force the war to conform to a template we understood (conventional war) led us to assume the enemy would view the war the same way. Never once during the entire course of the conflict were our senior leaders able to step into the enemy's shoes and see things as they did.[8] Even when study groups accurately identified the Vietcong as an insurgent force with only tenuous connections to the North, the strategy recommended was not aimed at countering an insurgency, but instead at a standard view of a partisan conflict guerrilla war with North Vietnam as an external sponsor and, therefore, as the main enemy. Such a recommendation left senior military leaders with a false sense of satisfaction, for it contained a recipe for victory using conventional tactics that they felt very well prepared to cook.[9]

The resulting Rolling Thunder air interdiction campaign against North Vietnam was not only misplaced, but counterproductive. The U.S. concentrated on a military solution which they felt would serve to demoralize the North. Instead, the bombing served to

harden the political resolve of the North Vietnamese, and only strengthened their ability to tolerate being bombed. Far from coercing Hanoi, the bombers invited the North to enter the war in pursuit of its own goals. Rolling Thunder had transformed the conflict from an insurgency to a partisan war, but not on the terms America had expected. The mobile U.S. strategy of 'find-fix-fight-finish' was supposed to minimize loss of American lives. North Vietnam, by being willing to accept large losses over an extended period of time in order to gradually inflict more and more losses on the U.S., was able to hang on until U.S. public opinion finally turned firmly against the war.[10] American political resolve finally gave out in 1973. In the end, U.S. strategic aims in Vietnam were overcome not by military force (the U.S. mindset) but through a campaign of intense political and psychological warfare waged by North Vietnam and its allies (their mindset), aimed at wearing down our political and moral resolve.[11]

The loss had a profound impact on the development of U.S. strategy following the war. While the other services, particularly the Army, were also affected, the Air Force underwent fundamental change in several areas. Wary of repeating another Vietnam, terms like *insurgency, counterinsurgency,* and *guerrilla warfare* were replaced with new ones like *low-intensity conflict.*[12] The Army, through its Training and Doctrine Command (TRADOC) teamed up with Tactical Air Command (TAC) to develop the AirLand Battle concept, again designed to fight something we were comfortable with, a conventional war in Europe against the Soviet Union and Warsaw Pact.

The Air Force, now under the leadership of the "Fighter Mafia," undertook development of air-superiority fighters, of intense training programs such as Red Flag, and of new missile programs to correct deficiencies noted in Vietnam—all aimed again

toward successfully prosecuting a conventional war and generally in a support role to the Army.[13] Yet despite all these changes, which were in fact useful in many respects, there was still a nagging sense among many who felt that there still existed no clear overall vision within the Air Force for employing these forces—that the real problem lay with the senior officers who failed to comprehend and articulate a unifying vision of airpower and the profession of arms (i.e., airpower theory).[14]

The Aftermath of the Cold War

The Reagan years instituted a major push to counter the primary threat we saw at that time: the military might of the Soviet Union. The U.S.-Soviet military competition was extremely expensive. While the U.S. may have won the Cold War, the rest of the nations of the world did not sit idly by. They were preparing themselves for round two—economic warfare. The U.S. was so preoccupied with military superiority over the Soviets that we generally allowed our economy to erode without noticing, until it has now reached a critical point. Future historians may consider outspending the Soviets as a very stupid move indeed.[15]

The end of the Cold War also led to other major changes. Potential global conflict between the two superpowers has been replaced by regional conflicts between comparatively small ethnic and political groups. The old notions of conducting small wars, distorted as they were, have become even less relevant. In many ways, the world was a much safer place in the bi-polar world of U.S. versus USSR. The lines were clearly drawn. We had our puppets, they had theirs, and we battled over which economic and political philosophy was better. Now, with no more Soviet-sponsored client states trading ideology for financial support, everyone is on his own.[16] Politically and militarily, future

U.S. dealings with military operations other than war (MOOTW) will be full of danger. The future is likely to be dominated by peace enforcement in failed states (such as Bosnia), different forms of "spiritual" or "commercial" insurgency (vice protracted guerrilla war), terrorism, and drug wars. Many Third World nation-states will fragment into smaller units. Ungovernability and instability will be the normal state of affairs, with power held among warlords, primal militias, and well-organized, well-financed politico-criminal organizations.[17]

Already in the aftermath of the Cold War, U.S. attention is requested around the world, stretching our resources to the limit. U.S. leadership is under the gun as we try to cope with global interests. We want to lead, but simply do not have the resources to be everywhere at once. This will force U.S. policy to be more selective.[18]

Why Information Wars Will Be Fought

Make no mistake about it: we are already at war in the struggle for information control. Information warfare is essentially about money, power, and survival.[19] Information wars will be fought for several reasons.

- The comparatively simple technology required for information warfare is universally available;
- America and Americans are still often viewed as spoiled, self-indulgent brats demanding instant gratification. That image makes us inviting targets;
- Only twenty-five percent of the planet can be considered developed, leaving several billion Have-Nots;
- Information warfare offers tremendous financial gain to the winner and devastation to the loser; the rules of the competition aren't the same for everyone—from both a competitive and combative perspective, in many respects, it would be stupid for a well-financed and motivated group *not* to attack the technical infrastructure of the U.S.;
- The effects of information warfare are unique in the annals of conflict; information warfare is a low-budget, high-tech vehicle for mass destruction;

- Information warfare is a low risk/high reward endeavor; because of the current situation of extreme vulnerability of computer systems, information warfare is a convenient vehicle of mass destruction for virtually anyone so inclined, from anywhere in the world;
- We increasingly rely on computers to sustain our society; the rapid increase in the number and quality of computers has created a global network that is rapidly redefining not only business relationships, but also the meaning of power; and
- Perhaps most importantly, information warfare will be waged because it can be. History clearly shows that any new technology, regardless of its original intentions, soon finds its way into the arsenals of the warriors.[20]

Environmental Components

The performance of essential national security-related activities depends more and more on a rapidly growing, supporting information infrastructure,[21] commonly known as the "Web," "Internet," or "Information Superhighway."[22] The Department of Defense (DOD) information infrastructure is embedded in larger and extremely complex national and global infrastructures. This section examines briefly the nature of this huge infrastructure; the legal, regulatory, and policy environment; emerging technologies; and adversary capabilities.

Information Infrastructure

The national security posture of the U.S. depends more and more on the National Information Infrastructure and the larger Global Information Infrastructure. Each of these information infrastructures is incredibly complex. Each relies on other infrastructures such as electrical power and energy. Over 95 percent of the worldwide telecommunications needs of the Department of Defense (DOD) travel over commercial telecommunications carriers, outside DOD control.

These information infrastructures are very vulnerable at the present time. Recently, electronic intruders have penetrated major U.S. telecommunications carriers and Internet service providers, many international organizations, and a wide variety of end-user systems. Intruders have included foreign intelligence agents, economic espionage agents, organized crime members, drug cartel members, private detectives, hackers, and insiders.

At present, there is no consensus among the various agencies and organizations of the United States concerning a national information policy that deals with such issues. The DOD is obviously concerned about this situation because of the security implications and its dependence on an information infrastructure over which it has little control. It has recommended to the National Security Council staff the need to initiate interdepartmental discussions concerning vulnerability and dependency issues, and the possible need for a national-level policy to deal with such issues. The Air Force, as a subset of DOD, faces this same threat from IW attacks, and must likewise rely on other organizations to protect its information and supporting infrastructures.[23]

In addition to the problems noted above, the rapid growth in this area has outpaced both the Federal Government and the private sector in several other respects. For example, there is no set of commonly agreed upon terms and definitions at the present time to permit a meaningful discussion of IW issues and how to resolve them. Figure 1 shows some of the terms currently in use.

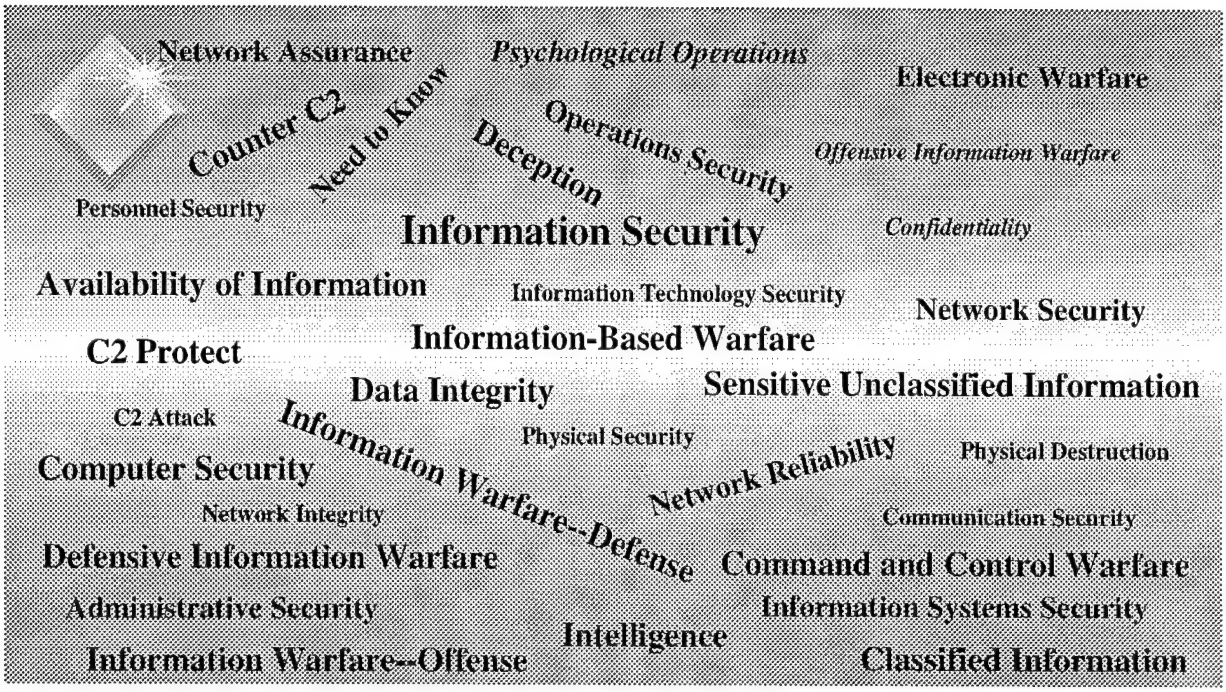

Figure 1. Common Information Warfare Terms in Current Use[24]

Another problem is that the perception of IW issues is strongly influenced on individual experiences and organizational missions and functions. For example, DOD might view an electronic intrusion into a financial network as a diversionary effort to aid in concealing more significant intrusions into its command and control structure, or as evidence of an attack on America, or as means to obtain funds to purchase weapons of mass destruction. The law enforcement community would view the same situation as an attempt to defraud of steal and would be focused on gathering evidence to prosecute the intruder. The commerce community might view it as an act of economic espionage and request the assistance of the FBI, which in turn might have different goals from the rest of the law enforcement community. The intelligence community might view the intrusion as an opportunity to gain intelligence about the intruder. And so on. As the saying goes, where you stand depends on where you sit.[25]

The list of other key problems includes but is not limited to the following:

- Responsibilities for information protection are not consistently assigned within Executive Branch departments;
- Most non-DOD organizations have no structure and process for the exchange of sensitive information over information networks;
- Most organizations have no capability to detect intruders, identify the nature of the intrusion, respond to intrusions, or recover from intruder disruptions;[26]
- Budget and staff to address IW-related matters are generally very limited;
- All organization are faced with constant change, which has direct implications on information security; and
- Executive-level understanding of IW issues is minimal but growing.27

Legal Environment

Proposals such as the Clipper chip, which would also monitoring by the Federal government of encrypted transmissions under very specially designated and controlled circumstances, has solidified in the minds of business, industry and civil libertarians that the government must be watched at all times.[28] Right to privacy is a central issue in IW.

In addition to ensuring citizens' rights, the Constitution charges Congress with the following responsibilities that are relevant to IW:

- ". . . securing for limited Times to Authors and Inventors exclusive Right to their respective Writings and Discoveries";
- "To define and punish…Offenses [sic] against the law of Nations;
- "To declare War";
- "To regulate interstate and foreign commerce";
- "To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers."

In the Constitution, we see the genesis of one of the more controversial issues related to IW, the conflict between a citizen's right to privacy, and the responsibility of the government to provide for the welfare and common good and ensure economic and national security.

Several key statutes apply to IW-related objectives. The objectives themselves can be broken down into four main areas:

- Protecting individual privacy and providing access to government information;
- Securing Federal information and information systems;
- Ensuring infrastructure availability and reliability; and
- Defining the criminality of computer fraud and abuse.

In general, Congress has chased technology for the last several years, and the number and types of laws related to IW is very extensive. As technological capabilities have increased, Congress also began defining new methods of exchanging information in which citizens could legitimately expect privacy. Today, unauthorized interception of communications is illegal for almost every type of electronic or wire communication, regardless of the type of information (e.g., voice, data, or video) or medium (e.g., cordless, cellular, or fiber optic) except for radio communications readily accessible to the general public. Any encrypted or scrambled information, even transmission techniques such as spread spectrum, are not considered readily accessible and therefore, unauthorized interception is illegal.

The Foreign Intelligence Surveillance Act of 1978 established a process to facilitate electronic acquisition of foreign intelligence within America, while at the same time minimizing on U.S. residents. Court orders are normally required, unless the Attorney General, acting on behalf of the President, certifies in writing the purposes and procedures to be employed in order to minimize the impact on U.S. residents.

The Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) have purview over certain types of clandestine operations during peacetime. The FBI is responsible for foreign counter-intelligence operations (monitoring foreign agents and

U.S. citizens for evidence of prohibited espionage activities) within the United States, while the CIA is the proponent for activities outside the United States. Foreign or domestic covert intelligence activities—which may include clandestine electronic intelligence gathering—require a Presidential intelligence finding, and must be coordinated with the CIA or FBI. Only the CIA can conduct special activities without a presidential determination. As an exception, the Armed Forces may engage in special activities in time of war as declared by Congress or after the President has reported to Congress in accordance with the War Powers Resolution Act.[29]

Despite the successful prosecution of Robert Morris, a Cornell University graduate student who released a computer worm across the Internet in 1988, most computer crimes go unpunished at the present time. The lack of prosecutions can be attributed to the fact that many computer crimes are committed by insiders. In addition, corporations are often reluctant to report computer crimes which might tend to erode the public faith. This is especially true for institutions primarily responsible for money, such as banks. There is also the perception that computer offenders cause no quantifiable loss to their victims, even though they obtain confidential information, may evade effective punishment under current Federal laws. Finally, there is the question of jurisdiction, which often transcends both state and national boundaries. International crimes must rely on bilateral and multilateral treaties and agreements. Generally, such agreements require *mutual criminality*; that is, an offense must be a crime in both countries for the foreign country to take action.[30]

Regulatory Environment

The Federal Government regulates industry and Federal information warfare activities in three ways: (1) by passing laws and issuing orders and regulations, (2) through the activities of regulatory agencies, and (3) through export control.

Orders and Regulations. Executive Orders are formal policy documents issued by the President which normally precede or implement law. Other documents such as Presidential Proclamations, Memoranda, and Directives are equally formal but have more specialized functions. Orders and regulations are designed to achieve many of the same basic goals of legislation, to include ensuring the availability of telecommunications infrastructure, regulation of communications facilities in the public interest, providing access to government documents, protecting certain classes of information from unauthorized disclosure (e.g., classified information), preservation of individual privacy, defining the limits of authorized and unauthorized behavior, and defining administrative responsibilities. The U.S. Code of Federal Regulations describes the legislative basis, goals, and predominant policies of the Federal Government. In effect, it implements law and Executive Orders.

Regulatory Agencies. These organizations affect the information infrastructure in many ways. Agencies include, among others, the FCC (regulation of the telecommunications industry), the Department of Justice (DOJ) (enforcement of antitrust laws in the telecommunications industry), and the Federal Trade Commission, the Interstate Commerce Commission, and the Nuclear Regulatory Commission (NRC) (all affect possible IW activities). The NRC, for example, requires utilities to have constant communications to nuclear power plants, loss of which could be a serious IW incident.

The FCC is the primary regulatory agency. Among its many duties, a key responsibility is ensuring the reliability of the Public Switched Network.[31] The "Switch" is perhaps the biggest network of them all, and generically refers to the phone networks that carry voice, and now digital, signals to almost every home in America. Once a hacker has access to the switch, he can eavesdrop on any conversation in the U.S.[32]

Export Control. Authority for export control is shared by the Department of State (DOS) and the Department of Commerce (DOC). The DOS is responsible for export of items designed primarily for military use, and maintains appropriate regulations and specific listings of items requiring a DOS license for export. The act charges DOD with providing recommendations to the DOS. The DOC is responsible for sensitive or dual-use products, to include software and scientific data, and maintains a list similar in purpose to that of DOS of controlled items. Export of cryptography is a very controversial political issue, involving discussions regarding national security, foreign policy, and national and global market forces.[33]

Policy Environment

There is currently no national policy on information warfare. However, the Executive Branch is actively involved in creating a large body of guidance in this arena. DOD has been in the forefront, producing policy documents for interagency consideration as the need has arisen. As previously mentioned, issues related to IW are interpreted in many different ways at the national level by the organizations concerned. A key factor contributing to the turbulence and complexity of the issue of developing a national IW policy is the dynamic nature of technology. Policy needs to be provided in such a way that technological changes do not result in major policy changes.[34]

In 1993, the Secretary of Defense and the Director of Central Intelligence established the Joint Security Commission (JSC) for the purpose of examining processes used to make and implement security policy in the respective organizations. The JSC observed that "the policies and standards upon which the Defense and Intelligence Communities base information systems security services were developed when computers were physically and electronically isolated. As a result, policies and standards are not suitable for the networked world of today. . . ."[35]

The Chairman, Joint Chiefs of Staff (CJCS), has similarly issued Instructions, Memoranda of Policy (MOPs), and Joint Publications. Joint Publication 1, *Joint Warfare*, refers to the "information differential." CJCS MOP 30, *Command and Control Warfare (C2W)*, gives joint policy and guidance for both the offensive and defensive aspects of C2W.

Emerging Technologies

Emerging technology will continue to have a major impact on both offensive and defensive IW. It involves all stages in the processing, transmission, storage, encryption and protection of information. Technology solutions are not limited to either hardware or software. Generally, there is a continuous and rapid tit-for-tat development of offensive attack measures versus defensive countermeasures. At the moment, the offense has the upper hand, however, increased awareness of the potential impact that IW can have on the national power is prompting a strong response.

Emerging technologies are being fostered by such efforts as the Joint Warfighters Capability Assessment, the Air Force Information Warfare Center, and research and

development in technologies which potentially have long-range IW applications.[36] Examples of such technologies include:

- Network sniffers and analyzers (generally for offensive IW),
- Network encryption, authentication, and watch dogs (for defensive IW),
- Packet filtering using firewalls and routers that filter network traffic and prevent undesirable traffic from reaching protected computers (defensive),
- Efficient communications protocols with increased throughput (allows faster transmission of information),
- Broadband and wireless communications, such as cellular phones (reprogramming cellular phones to bill innocent, legitimate users is a major money maker for organized crime),
- Van Eck radiation detection of the picture displayed on computer monitors (can be used to steal secrets, or by law enforcement authorities to monitor illegal activities),
- Chipping (building special chips that do more than advertised, e.g., Japanese integrated circuits produced for American cars could be made to fail after a predetermined delay, in order to gain competitive advantage over the U.S., and would be virtually impossible to detect),
- High energy radio frequency (HERF) guns and electromagnetic pulse transformer (EMP/T) bombs (both designed to transmit very powerful bursts of energy which destroy or incapacitate a variety of electronic targets), and of course,
- Viruses (offensive IW).[37]

Adversary Capabilities

According to Sun Tzu, "Thus it is said that one who knows the enemy and know himself will not be endangered in a hundred engagements. One who does not know the enemy but knows himself will sometimes be victorious, sometimes meet with defeat. One who knows neither the enemy nor himself will invariably be defeated in every engagement."[38] Information warfare has both offensive and defensive forms. To mount an effective IW offense, the adversary must be well understood. Defensive IW requires knowledge not only of potential adversary capabilities, but also a detailed understanding of one's own strengths and vulnerabilities. Having described the U.S. IW environment,

this chapter concludes with a brief examination of the adversary environment, describing the future adversaries the U.S. will likely face as well as their motives and types of attack.

Adversaries and Motives

Literally hundreds of traditional and non-traditional groups of people could be considered potential adversaries. Anyone with a computer, modem, and telephone can gain access to almost any portion of the information infrastructure from any location; detecting and tracing such activity can be extremely difficult with current technologies. Open sources admit, however, that several countries are actively targeting the U.S. using advance computer espionage techniques.

Often, this is done covertly, with organizations such as the KGB sponsoring groups such as the Hanover Hackers, who in turn were able to gain unauthorized access to more than two dozen computer systems that contained classified information, plus a host of other systems which did not. This is one of the rare cases when state-sponsored espionage has been acknowledged. Defense Information Systems Agency reports indicate a large number of intrusions continue, and that the scale of the attacks may be increasing.

Even nations considered friendly to America have admitted espionage against the U.S. In almost all of these cases, the stated goal was economic intelligence. Both the U.S. Government and U.S. corporations are targets. It would be wrong to assume that such economic intelligence gathering is not security related. Losses suffered by the United States are measured in billions of dollars annually. Stolen technologies are no longer controlled by U.S. export regulations, and are in turn passed on to U.S. military adversaries. Most important, the techniques used to gather economic data could just as

easily be used for disruptive purposes. Even if not targeted directly against the military, attacks could significantly disrupt our domestic economy and infrastructure, which in turn would delay or disrupt military functions, and could cause widespread secondary effects such as loss of power, telecommunications services, financial chaos, etc.

Other adversaries may desire to gain access to sensitive technologies or identify targets for terrorist attack. This category also includes organized crime, which is concerned with electronic theft, money laundering (especially the drug cartels), and extortion. Often, such organizations recruit expert help from individuals in financial difficulty. For example, the collapse of the Soviet Union left a number of very talented computer and communications professionals out of work and broke. They are facing their traditional enemy, only now they are much better paid.

Finally, there are numerous individuals and groups within the U.S. also quite capable of IW attacks. This could include anyone from teenage hackers to disgruntled former employees to militant groups. Many hackers do not feel they are doing anything wrong. What they fail to realize is that others who do intend harm are watching them closely as they learn new techniques to break into networks.

From a security perspective, hostile countries and terrorist organizations represent the greatest short-term threat to U.S. national security interests. Economic competitors are inclined to steal our secrets, but not likely to mount disruptive or destructive attacks on the national infrastructure.[39] Again, however, when viewed from another perspective even this theft of information can be dangerous to national security. In the industrial age, only tangible assets had value. In the information age, we must realize that non-tangible assets such as information have strategic value to the United States, and that when lost

cause a negative impact on the growth of the country, its economy, its global competitiveness, and the interests of its citizens and workers.[40]

Types of Attack

America's adversaries are currently able to compromise virtually any computer or communications information system that has connectivity to the outside world. A prime target is the Public Switched Network, which includes telephone systems and cellular communications systems. Since 95 percent of military communications are routed over commercial telephone lines, this poses a significant threat. Although theft of information can be prevented through encryption, the threat of denial of service is high. Crippling even part of the PSN could have a major impact on military communications.[41] Other examples include:

Logic attack, such as erasing or corrupting a database containing data needed for an offensive strike could compromise U.S. operations plans, e.g., modifying Time Phase Force and Deployment Data (TFPDD).

Physical attacks on infrastructure support such as buildings, power, environmental control units or fiber optic cables could result in the loss of a primary telecommunications link, cause significant loss of data and information, and isolate portions of a network; Corrupting key network management data could cause several networks to fail. Introducing viruses can cause a network to overload and break down at a critical juncture; and Physical and logic attacks could be combined to mask one or the other.[42]

Chapter Summary

This chapter examined several of the major factors affecting the IW environment. Three recent historical events were laid out to first set the stage, then examples were presented to show why information warfare is inevitable. Next, an overview of the various components of the IW environment was presented. Five of these environmental components: the information infrastructure; the legal, regulatory, and policy environment; and emerging technologies described U.S. capabilities and constraints. The final component described adversary capabilities. Having provided this broad discussion on information warfare as it relates to national security as a background, the next chapter will attempt to narrow the discussion in two respects, by examining how information warfare impacts on the Air Force, and its strategy for military operations other than war.

Notes

[1] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 18.

[2] Alvin and Heidi Toffler, *Creating a New Civilization, The Politics of the Third Wave* (Atlanta: Turner Publishing, Inc., 1995), 19.

[3] Ibid., 14.

[4] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), 11-12.

[5] Ibid., 12-13.

[6] Ibid., 47.

[7] Col Edward C. Mann III, *Thunder and Lightning, Desert Storm and the Airpower Debates* (Maxwell AFB, AL: Air University Press, April 1995), 11-12, quoting Harry Summers, Jr., *On Strategy: A Critical Analysis of the Vietnam War* (Novato, Calif,: Presidio Press, 1982), 21.

[8] Stephen Young, "How North Vietnam Won the War," Wall Street Journal, August 3, 1995, interview with Colonel Bui Tin, North Vietnamese army, as reprinted in the *Daedalus Flyer*, special reprint.

[9] Larry Cable, "The Operation Was a Success, but the Patient Died: The Air War in Vietnam, 1964-1969," from *An American Dilemma: Vietnam, 1964-1973*, by Dennis E. Showalter & John G. Albert, 1993, 128, as reprinted in *Air War College Department of Strategy, Doctrine and Air Power Readings*, Vol. 2, Academic Year 1996 (Maxwell

Notes

AFB, AL: Air University Press, October 1995), 379. Copyright 1993 by Imprint Publications.

[10] Ibid., pp. 125, 143, 149.

[11] Jerome W. Klingaman, "US Policy and Strategic Planning For Low-Intensity Conflict," from *Low-Intensity Conflict in the Third World*, compiled by Lewis B. Ware, et al. (Maxwell AFB, AL: Air University Press, August 1988), 164-165.

[12] Ibid.

[13] Richard P. Hallion, *Storm over Iraq, Air Power and the Gulf War* (Washington: Smithsonian Institution Press, 1992), pp. 27-54, 72-75.

[14] Mann, *Thunder and Lightning*, 186; also Carl H. Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force*, (New Brunswick, N.J.: Transaction Publishers, 1994), 3-4.

[15] Schwartau., *Information Warfare: Chaos on the Electronic Superhighway*, 38, 42.

[16] Ibid., 28, 30.

[17] Steven Metz and James Kievit, *The Revolution in Military Affairs and Conflict Short of War* (Carlisle Barracks, PA: Strategic Studies Institute, July 25, 1994), v, 3-4.

[18] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 28-29; also Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, v.

[19] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 15.

[20] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 20-22.

[21] Science Applications International Corporation (SAIC) Report to Joint Chiefs of Staff, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 4 July 1995, p. P-1.

[22] ———, "The 1,000 Best Web Sites," *PC Computing*, December 1995, 121.

[23] SAIC Report, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, p. 1-1.

[24] Ibid., p. 3-3.

[25] Ibid., p. 3-4.

[26] Ibid., p. 2-6. Recent tests by the Defense Information Systems Agency on logistics and medical systems showed that 88 percent of targeted computers could be penetrated, that only 4 percent of the successful penetrations were detected, and that only 5 percent of the detections were reported.

[27] Ibid., pp. 3-5, 3-6.

[28] Ibid., p. 3-4.

[29] Ibid., pp. 2-14 through 2-18.

[30] Ibid., pp. 2-26, 2-29.

[31] Ibid., pp. 2-41 through 2-43.

[32] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 122-124.

[33] SAIC Report, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, pp. 2-43, 2-44.

[34] Ibid., p. 2-51.

[35] Ibid., p. 2-53.

Notes

[36] Ibid., p. 2-57; also Steven Watkins, "New Era has Humble Start," *Air Force Times*, November 20, 1995, 24.

[37] SAIC Report, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, p. 2-57; also Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 114-189.

[38] Sun Tzu, *The Art of War*, from *The Seven Military Classics of Ancient China*, ed. and trans. Ralph D. Sawyer and Mei-Chun Sawyer, (Boulder, CO,: Westview Press, 1993), 162.

[39] SAIC Report, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, pp. 2-68 through 2-71.

[40] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 335.

[41] SAIC Report, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, pp. 2-69, 2-70.

[42] Ibid., pp. 2-6 through 2-8.

Chapter 3

Impact On Air Force IW Strategy for MOOTW

As a rule most men would rather believe bad news than good, and rather tend to exaggerate the bad news. The dangers that are reported may soon like waves, subside: but like waves they keep recurring, without apparent reason. The commander must trust his judgment and stand like a rock on which the waves break in vain. It is not an easy thing to do.[1]

—Carl von Clausewitz, *On War*

General

This chapter begins with a brief review of military operations other than war, to include its purpose and sub-categories (types). Next is a short discussion explaining the likelihood of MOOTW in future military operations. Following this, emerging IW applications that impact on MOOTW will be outlined. Certain types of MOOTW will require unique IW capabilities not currently planned for in conventional warfighting operations. Others can take advantage of many of the same IW capabilities available for conventional war, but generally to a lesser extent.

MOOTW Defined

Although the term "military operations other than war" is relatively new, the concept behind it has been around for quite some time, probably since the late 1950s or early 1960s, when the strategy of massive nuclear retaliation began to be replaced by one of

flexible response. The wide variety of military operations considered to fall under this term are both its greatest strength and weakness. The strength behind this mental construct lies in its flexibility. MOOTW can be applied to complement any combination of the other instruments of national power, encompassing the use of military capabilities across the range of military operations short of large-scale conventional combat operations.[2] The weakness is the sheer complexity it presents, which not only makes it difficult to truly understand, but also contributes to a general lack of advocacy when competing for budget dollars, as larger, simpler programs are naturally easier to focus on clearly.

MOOTW and war often seem similar in action, however, the primary focus of MOOTW is on deterring war and promoting peace, while war focuses on large-scale, sustained combat operations. MOOTW are more sensitive to political considerations; often the military is not the primary player. Also, rules of engagement are generally more restrictive than war, and broad national objectives, vice just military objectives, are adhered to closely.[3] The sixteen types of MOOTW can be broken down as follows:

1. Arms Control (e.g., START treaty verification)
2. Combating Terrorism (further broken down into *Antiterrorism* (defensive measures), and *Counterterrorism* (offensive measures)
3. DOD Support to Counterdrug Operations (e.g., establishment of JTF 6 in 1989 along Southwest border of U.S.)
4. Enforcement of Sanctions/Maritime Intercept Operations (e.g., sanctions enforcement in Operation SUPPORT DEMOCRACY of the coast of Haiti in 1993)
5. Enforcing Exclusion Zones (e.g., Operations SOUTHERN WATCH in Iraq in 1992, or DENY FLIGHT in Bosnia in 1993)
6. Ensuring Freedom of Navigation and Overflight (e.g., Berlin air corridor from 1948-1990, or the Gulf of Sidra operations against Libya in 1986)
7. Humanitarian Assistance (e.g., Operations SEA ANGEL I (1991) and II (1992) in Bangladesh following Cyclone Marian)

8. Military Support to Civil Authorities (e.g., deployment of troops to California in 1992 during civil disturbances)
9. Nation Assistance/Support to Counterinsurgency [This one starts to get tricky. Nation assistance includes civil or military assistance *other than* humanitarian assistance, designed to promote long-term regional stability. Includes things such as security assistance (e.g., Foreign Military Sales or International Military Education and Training Program), Foreign Internal Defense (political, economic, informational and military support to *assist* another nation fight subversion and insurgency), and humanitarian and civic assistance (must be done *in conjunction with* military operations and exercises, and must first fulfill unit training requirements that also just happen to create humanitarian benefit to local populations; e.g., medical and dental care, drilling wells, simple construction projects). Note than FID is broader in scope than support to counterinsurgency, which includes military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat *only* an insurgency]. Example of nation assistance: Operation PROMOTE LIBERTY in 1990, following Operation JUST CAUSE in Panama
10. Noncombatant Evacuation Operations (e.g., Operation EASTERN EXIT in 1991 (Somalia) or Operation QUICK LIFT in 1991 (Zaire)
11. Peace Operations [Another semi-tricky one. Includes peacekeeping operations (Sinai, since 1982, *with the consent* of the belligerents) and peace enforcement operations (latter stages of Somalia, 1992-1993, *without the consent* of the belligerents, to compel compliance and restore peace and order). Not to be confused with preventive diplomacy (diplomatic actions taken in advance of a predictable crisis), peacemaking (diplomatic settlement of a dispute), or peace building (post-conflict actions, generally diplomatic and economic, designed to avoid a relapse into conflict)]
12. Protection of Shipping (e.g., Operation EARNEST WILL, the reflagging of Kuwaiti ships in 1987)
13. Recovery Operations (of personnel, human remains, or black boxes, e.g., Operation FULL ACCOUNTING, the recovery of remains of U.S. service members lost during Vietnam)
14. Show of Force Operations (Big Stick diplomacy; involves appearance of a credible military force to stress U.S. policy interests, e.g., Operation JTF-Philippines in 1989 to support Aquino during a coup attempt against the Philippine government)
15. Strikes and Raids [(Example of a strike: Operation URGENT FURY in Grenada in 1983; offensive in nature, designed to accomplish a military objective for political purposes); (Example of a raid: Operation EL DORADO CANYON against Libya in 1986; generally smaller than a strike, and designed to get in and get out quickly)]
16. Support to Insurgency (Help a movement overthrow a constituted government, e.g., U.S. support to the Mujahadin resistance in Afghanistan during the Soviet invasion in the mid-1980s)

The above brief descriptions of the various types of MOOTW show two things clearly. First, as already mentioned, MOOTW covers a lot of ground—it is not simple. Second, virtually all the examples given have occurred in roughly the last decade. This leads to our next topic.

Why MOOTW Is Likely In Future Operations

Future conflicts will likely focus heavily on MOOTW, as opposed to mid- to high-intensity conventional conflicts or nuclear conflicts. No person or country in their right mind would take on the U.S. in a head-to-head military confrontation today. The Gulf War showed potential adversaries the superiority of U.S. forces for conventional combat. Saddam Hussein, with the world's fourth largest army, showed everyone what the Mother of All Defeats looked like.[4] America's capacity to project power is enormous. In Desert Storm, its air power was 20 times greater than that of the other two major Western participants (Britain and France).[5] There are simply much better ways to compete with the world's sole superpower. One of the best is MOOTW, which seeks to leverage asymmetries in which the adversary has advantages.

What is Asymmetric Warfare and How Does One 'Leverage Asymmetries?'

Asymmetric warfare is based on two key ideas that both run counter to standard Western notions of war. The first thought concerns the concentration of friendly strength against adversary weakness. The second idea is that of nonlinearity.

One of the best known of Clausewitz's ideas—the offensive thrust at the enemy's "center of gravity"—fits in nicely with the standard Western notion of pitting *strength*

against *strength*. Soldiers warm to the idea of focusing one's efforts on the most critical concentration of the enemy's fighting forces in order to strike the most telling blow.[6] As one recent example, Chairman of the Joint Chiefs of Staff General Colin Powell stated early in the planning for Operation Desert Storm, during discussions concerning the Republican Guard as a center of gravity, "I don't want them to go home. I want to leave smoking tanks as kilometer posts all the way to Baghdad."[7]

As a countervailing view, Sun Tzu, John Boyd and others stress concentrating *strength* against *weakness*. The basic strategy is to probe the enemy's organization and dispositions to unmask his strengths, weaknesses, patterns of movement, and intentions. Next, the enemy's perceptions are "shaped" to manipulate his plans and actions. Primary focus is on attacking first the adversary's plan, then his alliances, then his military, and finally his cities. Cheng (concerned with form, as well as spatial and fixed relationships) and Ch'i (dealing with formlessness, flexibility, and temporal relationships) maneuvers are then employed to quickly and unexpectedly hurl strength against weakness.[8]

"Nonlinearity" refers to something that is "not linear." Although this is obvious, what is not so obvious is the way the Western mind tries to make everything fit into linear models. Westerners prefer the "Keep It Simple, Stupid" (KISS)–principle approach, but sometimes it simply isn't possible to do this. The underlying notion is that "truth" resides in the simple (and thus the stable, regular, and consistent) as opposed to the complex (unstable, irregular, and inconsistent). For our Western intuition, this idealized approach can mislead us when the surrounding world and its messy realities do not fit this notion, something especially true in war and other forms of conflict. We like obedience to rules

and thus expected behavior—which places blinders on our ability to accurately see the world around us.

For a system to be linear two conditions must be met. The first is *proportionality*, which means that changes in system output are directly proportional to changes in system input. The second condition called *additivity*, which underlies the process of analysis. The central concept is that the whole is equal to the sum of its parts. This allows problems to be broken down into smaller pieces that, once solved, can be added back together to obtain the solution to the original problem. Nonlinear system fail to meet one or both of these conditions. They may exhibit erratic behavior through disproportionately large or small outputs, or they may involve "synergistic" interactions in which the whole is greater than the sum of its parts.[9]

Good adversaries will attempt to avoid U.S. strengths and attack our weaknesses, especially if they can advantage of the disproportionate effects or unpredictable situations generated by nonlinearities. Furthermore, war is not like chess; one's opponent does not always play by the same rules the U.S. does, and in the effort to win will often attempt to *change* what rules there are. This is a major reason that *how* a war is conducted can and does change its character, and that any war is structurally unstable.[10] Policy is not an independent variable with war the dependent variable; although policy *initially* determines how the war will be fought, it is itself subject to change as the war unfolds.[11] Perhaps a better way to view future conflicts is *not* as entities having a distinct beginning, middle, and end, but instead as part of a continuing cycle where policies and actions are formed, implemented, and evaluated over and over in a never-ending process.[12]

Future adversaries will likely seek asymmetrical countermeasures against the U.S., such as attacks on U.S. public support, terrorist attacks on U.S. forces to inflict high casualties, attacks on the will of our allies, use of low-technology countermeasures, damage to the economy, prolonged conflicts, attempts to deny us the moral high ground, and attacks to degrade command and control and other information systems. For anyone actually considering a fight against U.S. military forces, Indian Brigadier V. K. Nair has made several very pertinent observations. These include concentrated air attacks on 'critical soft targets' such as AWACS, JSTARs (both key IW assets) and air refueling tankers, which even if unsuccessful would compel these forces to operate at greater distances behind battle lines and thus degrade U.S. air activities. Special forces raids would be conducted against USAF forward bases and logistics concentrations. These teams would carry shoulder-fired SAMs (one of their best IW devices) to threaten air transport and other air movements. Above all, the potential opponent of the superpower would not passively await its fate as the Iraqis did. Although a purely military defeat of the U.S. might be impossible, it is still possible to raise American risks to an unacceptable level with actions that degrade U.S. command and control and quick thrusts that stay inside our OODA loop.[13]

Areas of MOOTW Which May Benefit from Emerging IW Capabilities

For the United States, the Gulf War marked a transition from industrial age to information age warfare, combining aspects of both types of conflict. It highlighted several problem areas caused by the flood of information associated with information warfare technologies. Information bottlenecks associated with areas such as command

and control, intelligence, and logistics have stimulated new discussions regarding the use of hierarchical versus networked organizations. Such discussions have applicability to both large-scale conflicts and MOOTW. In general, emerging IW technology will have less impact on MOOTW than on conventional conflict. In many cases, technologies designed originally for conventional conflict will be transferable to MOOTW. However, there are exceptions. Primary types of MOOTW which may benefit from emerging IW capabilities include, but are not limited to: support to insurgency/counterinsurgency, combatting terrorism (both anti- and counterterrorism), DOD support to counterdrug operations, peace enforcement operations, shows of force/raids/strikes, peacekeeping operations, non-combatant evacuation operations, nation assistance, freedom of navigation enforcement, humanitarian assistance, protection of shipping, and support to U.S. civil authorities.

The remainder of this section reviews the issue of organization, then examines each of the primary types of MOOTW noted above in turn.

Hierarchical versus Networked Organizations

Following Vietnam the U.S. made major upgrades in a number of areas, such as weapons and training,[14] but at least two key IW-related areas require re-thinking for future third wave conflicts, whether these conflicts are large or small. These areas are command and control (C^2) and intelligence. The Gulf War showed what will happen to nation states such as Iraq who choose to fight second wave, industrial-age warfare against nations such as the U.S. learning to fight third wave, information-age based warfare. Literally from the beginning of the conflict, the U.S. controlled the information and hence

the war. However, against more sophisticated opponents the story could be quite different.

Command and control was considered a key U.S. strength in the Gulf War, but it could just as easily have been a targeted center of gravity against a smarter adversary. Consider, for example, the impact which an accurate Scud attack[15] or an enemy special forces team could have had upon the war effort had they made an early infiltration into Saudi Arabia and killed the key U.S. planners working in the Black Hole in August of 1990. A key U.S. vulnerability was overcentralization, using a traditional pyramid-type hierarchical structure.[16]

In the intelligence arena, the U.S. and coalition faced a rather unique problem, not the usual one of having too little data, but of having too much. Somewhere, somehow, someone must process all this raw data into information and then knowledge that is useful to decision-makers. One need not do this perfectly, as Boyd has noted, only faster than one's adversary. The ability to discriminate between useful information and background "noise" (i.e., orientation) may have been the weakest link in the C^3I system used by coalition forces in the Gulf War. Intelligence delivered "tons" of information continually as fast as possible (their self-imposed measure of merit), but operations wanted "pounds" of it delivered more quickly than the system would allow. Unsatisfied operations planners resorted to unofficial work-arounds outside the normal system to get what they wanted.[17]

Both the command and control and intelligence weaknesses noted above are closely related in one important respect: stovepiping of the information flow to decisionmakers. Although U.S. technology has produced superb computer and communications systems to

aid decisionmaking on the battlefield, better doctrine is needed to organize this technology and exploit its full potential.[18] Since this problem is likely to be encountered over and over again in third wave information age warfare, whether full scale or MOOTW, a solution is needed to avoid being "out-OODA'd" by a wise adversary who knows how to exploit our information bottlenecks, disrupt our processes, and keep his own communications from being disabled significantly.

One possible solution calls into question the Air Force's most sacred tenet of aerospace power: centralized control and decentralized execution.[19] Both the command and control and intelligence problems may be solvable using a combination of hierarchical *command* structures together with fully networked information gathering *(control)* systems. The end result would be *centralized command*, but *decentralized control and execution.*

Networked organizations are ideal for information gathering which is essentially a control, or feedback, mechanism in the OODA loop (specifically, steps 1 and 2, *observe* and *orient*). However, combat command (steps 3 and 4 of the OODA loop, *decide* and *act*), by the very act of ordering forces to fight and often die, must be hierarchical in nature. Who, in a purely networked organization, would be able to make the difficult decisions required to order men and women into high-risk situations? War requires commanders, not coordinators or collaborators. Also, certain operations, such as major deceptions, require restricted access to a very limited number of people to ensure security and achieve surprise. Without even intending to do so, forces behave differently if they become aware they are part of a feint and won't really be used for serious combat action.

Power at each level of command within a hierarchical organization can be viewed as a function of how much and what kind of information one controls. However, under the current system, the very act of controlling information defeats the optimum use of that information. As data is collected by a host of sensors in the various levels of a hierarchical organization, it must be interpreted to give it meaning. Data (observed phenomena) becomes information through observation and analysis (steps 1 and 2 of the OODA loop).[20] As noted previously, this is fundamentally an intelligence function. This gathered data must work hard to get through many levels of command. In the process of becoming transformed from data into information, it must be filtered. This is not only a time-consuming process, but means that often key data is omitted or distorted as it travels from one level of an organization to the next, similar to the game we used to play as children wherein a story was whispered from one child to the next, and became more and more convoluted as it worked its way along the chain. The end result is exactly the opposite of that desired by a well-functioning command and control system. The crux of winning vice losing is the *relative* movement of opponents through their respective OODA loops. The winner will be he who repeatedly observes, orients, decides, and acts *more rapidly and accurately* than his adversary.[21]

A better structure for the rapid and accurate dissemination of information is the network. With the truly revolutionary advances occurring in information technology today, huge amounts of data can now be collected and made available to all commanders at all levels simultaneously (note that "huge amounts of data" does *not* mean all data—there will always exist certain data that must, for a variety of reasons, remain in restricted channels). Technology now also makes possible the design of *filters* which allow

commanders at each level to extract rapidly *only* the information required by their respective level of command. The commander at each level may choose to do this directly on occasion, but generally this will require the data manipulation talents and skills of a supporting intelligence staff, working closely with the operations staff. This simultaneous "push-pull" concept is already in the process of being developed at the strategic and operational levels (down to Joint Intelligence Centers), but due to funding constraints has not been carried down to tactical levels of organization yet. Such a network also provides redundancy (increasing survivability) and allows commanders to share a common topsight vision of the battlefield, automatically covering for one other as casualties occur.

Having examined the question of organization briefly, let us now turn our attention to how IW technology might be applied to various types of MOOTW.

Support to Insurgency/Counterinsurgency

The military objectives of insurgency and counterinsurgency are conversely opposed to one another. In support to insurgency the U.S. aid an organized movement attempting to overthrow a government opposed to U.S. interest. In support to counterinsurgency, the U.S. aid governments attempting to fight insurgents.[22] Information warfare technology can assist both efforts in a number of ways.

In supporting insurgency, U.S. forces recruit, organize, train and equip forces; develop institutions and infrastructure, gather intelligence; and perform psychological operations, surreptitious insertions, linkup, evasion, escape, subversion, sabotage and resupply. IW technology can be applied to simulator training devices to help with force development and to practice field-training problems. Unmanned aerial vehicles (UAVs)

can be used to conduct psychological operations to gain support and enhance the legitimacy of the insurgents. Stealth technology can be used for insertions, and sensor networks can provide intelligence support.

Support to counterinsurgency efforts will be similar in many respects. The desired goal is to gain and maintain government legitimacy. Intelligence requirements will be very high. Many emerging IW capabilities may be well suited to developing desired emotions, attitudes or behavior. Standoff weapons (with information supplied by the U.S. to the host government) could prevent outside support to insurgents without requiring a U.S. physical presence. Security forces could receive simulator forces to enhance their effectiveness, increasing public trust in the government's ability to provide adequate security, again directly related to maintaining legitimacy.[23]

As another simple example of the benefits to MOOTW that are possible from emerging IW capabilities, consider Foreign Internal Defense (FID). As previously mentioned, FID involves political, economic, informational and military support to assist another nation in its fight against subversion and insurgency. The U.S. could use its strong superiority in the information arena to provide friendly governments with the knowledge necessary to move quickly against insurgencies and subversive elements. Simply put, the U.S. supplies advisors armed with appropriate information, while the friendly government supplies the bulk of firepower and manpower.

Combating Terrorism

Providing safety is a primary goal when combatting terrorism. Emerging IW technologies can be used both for and against terrorism.[24] Examples include precision standoff weapons or intrusive information technologies such as Van Eck detectors, which

have been used by both law enforcement authorities and terrorist groups to spy on one another.[25] Americans stationed overseas are generally at higher risk than those stateside. If technology allows a reduced U.S. presence overseas, antiterrorism (defensive measures against terrorism) will be easier. Improved sensors and guard systems may make installations more difficult to penetrate. In counterterrorism (offensive measures against terrorism), precise personal intelligence can be more critical than precision-guided munitions.[26] Recent advances in electronics and sensors and the ability rapidly fuse intelligence data may now provide this precious commodity. New computer software can quickly discover and expose suspicious activities that would otherwise go undetected.[27] UAVs could be used to follow terrorists, so they could be targeted for attack by counterterrorist forces.[28] Aerial capability may soon exist to broadcast and alter television signals, removing or reducing a key terrorist weapon—media coverage.[29]

DOD Support to Counterdrug Operations

As in combating terrorism, counterdrug operations are primarily a law enforcement function, with the military providing support, and with intrusive information technologies used heavily by both sides.[30] Soft kill weapons such as HERF guns and EMP/T bombs could be used to interdict narcotrafficking flights by damaging or destroying their avionics.[31] Because narcotraffickers operate like terrorists, much of the same IW technology can be used against them. In fact, because they are so well funded, narcotraffickers are even more likely to rely on radios, cellular phones, fax machines and computers, greatly increasing their vulnerability to electronic intelligence gathering and disruption. One area of recent law enforcement focus in this regard is remote intrusive monitoring of the financial computer networks of offshore banks, in order to identify

deposits connected with money laundering.[32] In general, however, because the drug cartels are themselves closely networked organizations, they adapt quickly to law enforcement efforts. This, coupled with their ruthlessness, superior funding and equipment, make them very formidable opponents. A "Take the silver or take the lead" approach usually gets them what they want.

Peace Enforcement Operations

The primary objective of these operations is to compel compliance with resolutions or sanctions designed to maintain or restore peace and order.[33] Soft kill systems can play a key role. Advances in electronics and robotics could prove useful, allowing commanders to separate forces with a "no man's land" populated by remote sensing devices or robotic patrols and enforced with stand-off precision strike weapons, helping to keep peacekeeper casualties down and improving the odds that the peacekeeping force will remain long enough for a political resolution of the conflict.[34]

Shows of Force/Strikes/Raids

Shows of force are designed to demonstrate U.S. resolve and involve increased visibility of U.S. deployed forces in order to defuse a situation. Strikes are offensive operations conducted to inflict damage on, seize, or destroy an objective for political purposes. Raids are usually small-scale operations involving swift penetration of enemy territory to secure information, confuse the enemy, or destroy installations, followed by rapid withdrawal.[35] All make use of identical IW technologies developed for conventional war, since they are essentially mid- to high-intensity operations writ small. Terrestrial, aerial, and space-based, autonomous, wide-ranging, high-speed collecting

devices will identify precise targets and provide near-real-time information about adversary dispositions. Simulations will train forces and be used to rehearse attacks. Automation-assisted C^3 systems will synchronize and control stand-off precision-guided weapons systems in near-simultaneous attacks. And IW technology will be used to conceal the attacks and provide feedback on success following the strike.[36]

Noncombatant Evacuation Operations

As the United States becomes more integrated into the global economy, more and more American citizens may find themselves in areas of instability and conflict. As a result, voluntary and involuntary noncombatant evacuation operations (NEOs) will become more frequent. These operations are designed to relocate threatened noncombatants from a foreign country.[37] The main problems of NEOs are identification and notification of individuals, identification of safe routes out of country, and threat assessment. IW technology could be used to manage these problems more easily. U.S. citizens in remote locations could be equipped with individual position locator devices, or simply with cellular phones to allow prompt contact. In many instances, this could be used to avoid dangerous, last minute evacuations all together, by encouraging voluntary departure prior to a crisis. This could also reduce to need to "go public" in announcing the NEO, giving U.S. decision-makers more options in a developing situation. UAVs could be used to provide reconnaissance of possible evacuation routes and identify threats during the evacuation. When a NEO required combat action, standoff precision-guided weapons could greatly reduce the number of military members exposed to risks.[38]

Chapter Summary

This chapter transitioned from a broader discussion of information warfare national security issues to the more specific ones faced by the Air Force in regards to military operations other than war. It described current doctrinal concepts behind MOOTW, the types of MOOTW, and why such operations will be more likely in future conflicts. It then highlighted key issues which need to be resolved in command and control and intelligence, and some of the emerging IW applications that will probably have an impact on MOOTW, stressing that IW capabilities available for conventional war will generally not be as applicable to MOOTW. The next chapter will examine some of the major constraints limiting the development of an Air Force IW strategy for MOOTW.

Notes

[1] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 1976, 117.

[2] Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Military Operations Other Than War* (Joint Publication 3-07) (Washington: GPO, 16 June 1995), pp. 1-1, 1-2. Hereafter referred to as Joint Pub 3-07.

[3] Ibid., p. vii.

[4] Ibid., 28.

[5] Tony Mason, *Air Power: A Centennial Appraisal*, Chapter 8, 1994, 238, as reprinted in *Air War College Department of Strategy, Doctrine and Air Power Readings*, Vol. 3, Academic Year 1996 (Maxwell AFB, AL: Air University Press, November 1995), 15. Copyright 1994 by Brassey's (US), Inc.

[6] Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security*, Vol. 17, No. 3 (Winter 1992/93): 84. This superb article's central thesis is that Clausewitz understood clearly that war is far too complex to be boiled down to a few simplistic principles. Hence, our ability to predict the course and outcome of any given conflict is severely limited.

[7] Col Richard T. Reynolds, *Heart of the Storm, The Genesis of the Air Campaign Against Iraq*, (Maxwell AFB, AL: Air University Press, April 1995), 72-73, quoting Lt Gen Robert M. Alexander, Washington, D.C., transcript of interview with Lt Col Suzanne B. Gehri, Lt Col Edward C. Mann, and author, 30 May 1991, 33, Desert Story Collection, U.S. Air Force Historical Research Agency, Maxwell AFB, AL.

Notes

[8] Sun Tzu, *The Art of War*, 77-79. See also John R. Boyd, "A Discourse on Winning and Losing," August 1987, 13, unpublished set of briefing slides available at the Air University Library, Maxwell AFB, AL and Grant T. Hammond, lecture notes from Air War College Class 4401-A, *Making Strategy for the 21st Century*, 26 March 1996.

[9] Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," 61-62.

[10] Ibid., 74-75.

[11] Clausewitz, *On War*, 92: "the original political objects can greatly alter during the course of the war and may finally change entirely *since they are influenced by events and their probable consequences*." [Emphasis in original]

[12] Grant T. Hammond, lecture notes, 26 March 1996.

[13] Ibid., 242. Also Grant T. Hammond, lecture notes, 28 March 1996.

[14] Hallion, *Storm over Iraq, Air Power and the Gulf War*, 27-54, 72-75.

[15] William D. Smith, "Weapons Proliferation, There Is No More Vital Research Than That Involving Defenses Against Theater Ballistic Missiles," *The Almanac of Sea Power 1996*, Vol. 39, no. 1, (January 1996): 58. In this article, the author notes that modern versions of the Scud missile possessed by Middle Eastern countries, China and North Korea are far more capable than that which terrorized Israel and Saudi Arabia during Operation Desert Storm.

[16] The author is deeply indebted to Lt Col Greg Roman for much of the information contained in this section, especially his thoughts on the information and decision cycles contained within the Observe-Orient-Act-Decide (OODA) Loop developed by Col John Boyd, and his thoughts on centralized command, decentralized control and execution.

[17] Mann, *Thunder and Lightning*, 153, 156.

[18] John Arquilla and David Ronfeldt, "Emergent Modes of Conflict," *Cyberwar is Coming!*, RAND Corporation, 1992, as reprinted in *Air War College AY 1995-1996 Conflict and Change Reader* (Maxwell AFB, AL: Air University Press, Aug 1995), 377. Copyright 1992 by the RAND Corporation. The authors argue convincingly that technology permeates war but does not govern it. It is not technology in and of itself, but rather the *organization* of technology, broadly defined, that is important. They consider the combination of technology and this broad view of how to organize it as being at the heart of the information revolution that will bring the next major shift in the nature of conflict and warfare.

[19] Headquarters, Department of the Air Force, *Basic Aerospace Doctrine of the United States Air Force* (Air Force Manual 1-1), 2 vols. (Washington, GPO, Mar '92), 1:8. Hereafter referred to as AFM 1-1.

[20] Headquarters, Department of the Air Force paper, *Cornerstones of Information Warfare* (Washington, GPO, released in Fall of 1995 but undated), 2, hereafter referred to as Cornerstones.

[21] Major David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell AFB, AL: Air University Press, February 1995), 16. Thesis presented to the faculty of the School of Advanced Airpower Studies, Maxwell AFB, AL.

Notes

[22] Joint Pub 3-07, *Joint Doctrine for Military Operations Other Than War*, p. III-15; also Headquarters, Department of the Army and the Air Force, *Military Operations in Low Intensity Conflict*, Field Manual (FM) 100-20/Air Force Pamphlet (AFP) 3-20, Washington, December 5, 1990, p. 2-0 and pp. 2-7 to 2-9.

[23] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, 10-11.

[24] Ibid., 8-9.

[25] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 231-232.

[26] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, 157.

[27] Ibid.

[28] Ibid., 113.

[29] Chuck de Caro, "Sats, Lies, and Video-Rape: The Soft War Handbook," unpublished paper, Aerobureau Corporation, 1994, 32-34.

[30] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 231-232.

[31] Ibid., 171-176.

[32] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, 9.

[33] Joint Pub 3-07, *Joint Doctrine for Military Operations Other Than War*, III-13.

[34] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, 10.

[35] Joint Pub 3-07, *Joint Doctrine for Military Operations Other Than War*, III-14 and III-15.

[36] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, 5-6.

[37] Joint Pub 3-07, *Joint Doctrine for Military Operations Other Than War*, III-11.

[38] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, 6-8.

Chapter 4

Limitations on Air Force IW Strategy for MOOTW

There are a number of constraints on applying the [revolution in military affairs] to conflict short of war. These include the lack of a powerful institutional advocate for this process, a shortage of money for the development of technology specifically for conflict short of war, and the possibility that new technology may run counter to American values.[1]

—Steven Metz and James Kievit
The Revolution in Military Affairs and Conflict Short of War

General

New IW technology can improve the Air Force's ability to apply force in MOOTW, but the changes possible will not be as great as those for large scale combat operations. This is true for two reasons: the internal constraints we place on ourselves as a nation, and the external constraints placed on MOOTW by our opponents as they adapt to our strategy.

Internal Constraints

Internal constraints can be traced to two primary areas: institutional or legal and moral.

Institutional Constraints

The end of the Cold War has invalidated many concepts related to MOOTW. For example: insurgency/counterinsurgency doctrine is largely a product of the Cold War. Little attention has been paid to re-examining previous assumptions to see if they are still valid. Paradoxically, the successful end of the Cold War has stifled innovation in this area at the very time it is badly needed. The attitude of most is "if it ain't broke, don't fix it." The fact that the Air Force has not been confronted with a recent military disaster (indeed, quite the contrary, was largely the hero in Operations Desert Shield and Desert Storm) has hampered development and application of new IW technology to MOOTW. Primary Air Force attention regarding emerging IW strategy has largely ignored MOOTW and remained focused on mid- to high-intensity conflicts, for three reasons:

1. Lack of advocacy for MOOTW ("We sure as heck don't want to get into another Vietnam").
2. Reduced budgets. Both civilian and military leaders fear (probably rightly so) that time, effort, and of course dollars spent on MOOTW will be subtracted from that available for conventional warfare. Like a business investment in a new plant, military technology increases effectiveness and efficiency in the long term, but it has major short-term costs. With a reduced budget resulting from the end of the Cold War leaders must make some difficult choices, and tend to focus on the near term at the expense of mortgaging the future.
3. A feeling that much of the IW technology developed for mid- to high-intensity conflict will also have applicability to MOOTW. Fortunately, much of this technology can be used in this fashion, but certain areas such as insurgency, terrorism, and narcotrafficking will demand some unique capabilities.[2]

Moral Considerations

Two of the major moral issues now confronting us in the IW arena stem from recent technological advances which allow: (1) skilled individuals and organizations to actually steer the thinking of our adversaries, and (2) spying on the rest of the world to a degree never before possible.

Neocortical Warfare: The Acme of Skill

Quoting Sun Tzu: "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[3] The target of information warfare is the human mind, especially the mind of key decision-makers.[4] The decision-making process has been described by John Boyd's observe-orient-decide-act (OODA) loop feedback model. In this model, Boyd contends that the essential task of any decision-maker in a competitive environment is to observe, orient, decide and act faster (and more accurately) than adversaries. This faster tempo makes us appear ambiguous (unpredictable), thus generating confusion and disorder among our adversaries. The net effect is strategic paralysis, since our adversaries will be unable to generate mental images or pictures that agree with the faster patterns and decisions they are competing against.[5]

With the advent of new technology allowing the creation of fictive (subtlely biased, e.g., CNN news broadcast) or fictional (e.g., "morphed" virtual news conferences) universes[6], the issue now is not so much operating faster than an opponent as it is *controlling* the information contained in the opponent's OODA loop. Speed alone is not the goal. Shaping the *actions* of the adversary by forcing adversary *decisions* down a set of known or expected logic paths using knowledge of the adversary's *orientation* while controlling what the adversary *observes* is now possible with information warfare.[7]

A key question which must be addressed early in any discussion of IW regards whether or not using the techniques now available with emerging IW technology are compatible with American values and principles.[8] Is it acceptable to conduct "neocortical warfare" that strives to control or shape the behavior of adversary organisms, but without

destroying the organisms—in effect regulating the consciousness, perceptions and will of the adversary leadership: the adversary's neocortical system?[9] We may be very wise to decide not to start down this very slippery moral slope. Mind-control is definitely not a core American value, and one of the United States' primary means of influence in the international community has traditionally been our ability to maintain the moral high-ground. The slightest slip in this area would cause both national and world media to have a field day at American expense. Perhaps Boyd was right. Maybe just concentrating on faster OODA loops is good enough.

Offensive IW capabilities can also be used in a variety of ways that do not give the impression of mind-control, yet still provide the U.S. with operational advantages over an adversary. For example, development of capabilities which automatically identify, locate, and destroy the hardware and software of individuals and organizations attempting to steal military and economic information from the U.S. would probably be considered acceptable behavior by most of the world community, as it is retaliatory and not preemptive in nature. It sends a clear signal to intruders, and in addition to making them pay a price in terms of lost equipment, could also lead to prosecution or embarrassment in the world community. In any event, moral considerations implicit in IW are an area that deserves very careful thought up front, not after the fact.

Should We Spy on the World?

After all, they are clearly doing it to us. Theft of proprietary business information by foreign sponsored groups is up 400 percent since 1985. Shouldn't we try to level the

playing field a little by returning the favor? There are essentially three schools of thought on this topic.

The first school says, "Absolutely! It's spy versus spy versus spy and we should be playing the game harder. With the end of the Cold War, huge intelligence assets formerly used against the Soviet Union are now in search of a mission, so let's use them productively. It's time to fight back."

The second school says, "Wait! That's cheating, and besides, we're Americans. We can't announce to the world that we've allowed ourselves to be dragged down to their level of tactics. We have to play by the rules." The question, of course, is, which rules? Military spying has generally been considered acceptable, but what about economic spying? Spies have been generally been willing to put their lives on the line for their country, but would (and should) they do it for IBM or General Motors?

The third school says, "Have you checked out Cyberspace closely lately? Most of the answers you seek are begging to jump in your lap without having to play spy games. Just look!" This school contends that information is now an almost inexhaustible resource that can easily be tapped through the global information infrastructure, providing most of what the U.S. needs to make informed decisions.[10]

If the U.S. chooses to engage in MOOTW, two things could help to develop and apply new technology. First is the emergence of active and powerful supporters. Second is defeat or disaster. Yet even if America could make a strong effort to apply emerging IW technology to MOOTW, our opponents would quickly develop countermeasures.[11]

External Constraints

Since U.S. involvement in MOOTW will most likely continue to have weak domestic support, opponents do not have to match us innovation for innovation. All they really need to do is increase the cost of American involvement beyond the U.S. public and Congress' low levels of tolerance in this arena (again, largely due to Post-Vietnam syndrome). How, specifically, might they do this? In three ways: by striking at domestic support, by targeting friends and allies, and as a last resort by directly countering American forces.

Attacking Domestic Support

Adversaries will strike first at domestic support. One way, of course, is to kill Americans or damage U.S. property. Traditionally, this has been accomplished overseas. But in the ever more mobile and interdependent world of the information age, the United States itself will become increasingly vulnerable, as evidenced by the recent World Trade Center bombing in New York. Electronic terrorism—sabotage of communications and computer systems in retaliation against official U.S. policies, will also become commonplace. Finally, adversaries will undercut domestic support by political mobilization of immigrant and resident alien communities, as well as sympathetic indigenous political groups. A recent example is Muslim leader Louis Farrakhan's visit to leaders in Libya and Iran and his comment while in Tehran: "You can quote me: God will destroy America by the hands of Muslims."

Attacking Friends and Allies

Opponents will also counter U.S. military expertise by targeting our friends and allies. For American strategy to work in Third World nations, we must have a local ally with some base of legitimacy. Knowing this, future opponents do not have to confront U.S. forces and all their technological wizardry—all they need do is attack much weaker allies. Vietnam and the incompetent Saigon regime was an excellent example of this. In most types MOOTW, the host nation is the centerpiece of efforts to establish legitimacy. This is especially so, for example, in providing support to counterinsurgency, combatting terrorism, or support against narcotraffickers. The U.S. effort will be no more effective than its allies in such situations. Terrorists, insurgents and narcotraffickers will be the first to recognize this and will adapt accordingly.

Directly Confronting U.S. Forces

As a final resort, our adversaries will attempt to directly counter-deployed U.S. forces. They will attempt to counter U.S. technological abilities to locate and track enemy forces and to provide intelligence data by strategic, operational and tactical camouflage and deception. Opponents with external sponsors may receive enough technology to foil our forces, just as Stingers did for the Afghan mujahedeen. Others will take a low-tech approach, such as abandoning electronic communications in favor of written or voice messages, or relying on cellular terrorist organizations to thwart our intelligence gathering efforts. Adversary organizational decentralization will not destroy the effectiveness of our IW technology, but it will certainly degrade it.

Chapter Summary

This chapter briefly describes the chief constraints affecting the Air Force's ability to apply force using information warfare technology in MOOTW. Internal constraints are institutional and moral in nature. External constraints will include attacks against the U.S. domestic support base, our friends and allies, and as a last resort by direct confrontation with U.S. forces. This completes the detailed discussion and leads us to some final general conclusions and recommendations.

Notes

[1] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, vi.

[2] Ibid., 12-13.

[3] Sun Tzu, *The Art of War*, 77.

[4] George J. Stein, "Information Warfare," *Airpower Journal*, Spring 1995, 32.

[5] John R. Boyd, "A Discourse on Winning and Losing," 5. See also Major Jason B. Barlow, *Strategic Paralysis, An Airpower Theory for the Present*, (Maxwell AFB, AL: Air University Press, February 1994), 14-17, thesis presented to the faculty of the School of Advanced Airpower Studies, Maxwell AFB, AL; and Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, 16-17.

[6] Stein, "Information Warfare," 33-35.

[7] Robert J. Wood, "Information Engineering, The Foundation of Information Warfare," Air War College Research Report, April 1995, 5.

[8] George J. Stein, "Information War—Cyberwar—Netwar," Fall 1995, unpublished paper for seminar use in Air War College Course 2104-B, *Information Warfare*, 9.

[9] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," *Military Review*, November 1994, 47.

[10] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 337-339.

[11] Metz and Kievit, *The Revolution in Military Affairs and Conflict Short of War*, 13.

Chapter 5

Conclusions and Recommendations

> *War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied.*[1]
>
> —Sun Tzu, *The Art of War*

The impact of the information revolution will almost always be less on military operations other than war that it is on large-scale combat operations. The military dimension of MOOTW is likewise smaller as its primary focus is on deterring war and promoting peace. On the other hand, MOOTW are significantly more sensitive to political considerations, and often the military may not be the most important player. Political, diplomatic, cultural, psychological, and economic factors matter in all conflicts, but are key in MOOTW.

Proper control of information is key to future American security and competitiveness. Our current approach to MOOTW is a relic of the Cold War. The advanced technological nature of U.S. military forces and heavy reliance on computers makes them extremely susceptible to information attacks by a host of various groups such as nation states, multinational organizations, terrorist groups, and computer hackers. These new demand new ideas—the old assumptions must be challenged. To understand

and control the future, much greater research, analysis and debate is needed. New force structure, doctrine, organization and procedures should follow, not precede this debate.

A national information policy must be reached through a broad dialogue of all agencies and organizations, fully integrating the political, economic, military and informational instruments of national power. This is a critical task requiring immediate attention. The Air Force must continue to stress the development of leaders who understand the full impact of today's changes. This will require a major effort at all levels, from school house to flight line to command headquarters. These leaders will need to ensure they have the requisite skills needed to absorb new information technologies quickly.

Joint strategy must be part of a coherent national strategy for conducting information operations. The same considerations described above for Air Force leaders apply equally to joint personnel. The DOD must push other agencies in the federal government to correct deficiencies that are beyond its purview to address directly.

The legal, regulatory, policy, and especially moral dimensions of IW strategy for MOOTW must be examined carefully and up front. Ethically, the strategy must be consistent with basic American values or it will never work. A cost-benefit analysis must be performed *before* attempting to apply new technologies. Strategic considerations of MOOTW, rather than fascination with technology and enthusiasm for change, must be paramount.

Due to the rapid development of computer technology, proliferation of networked computer systems, and increased sophistication of adversaries, this is a very volatile area. Expect to rethink strategy and rewrite IW/MOOTW doctrine more than once.

Notes

[1] Sun Tzu, *The Art of War*, 63.

Bibliography

———. "The 1,000 Best Web Sites," *PC Computing*, December 1995, 121.

AFM 1-1. *Basic Aerospace Doctrine of the United States Air Force.* Vol. 1 of 2, Washington, GPO, Mar 1992.

Arquilla, John and David Ronfeldt. "Emergent Modes of Conflict," *Cyberwar is Coming!*. RAND Corporation, 1992, as reprinted in *Air War College AY 1995-1996 Conflict and Change Reader.* Maxwell AFB, AL: Air University Press, Aug 1995, 377.

Barlow, Major Jason B. *Strategic Paralysis, An Airpower Theory for the Present.* Maxwell AFB, AL: Air University Press, February 1994.

Beyerchen, Alan. "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security*, Vol. 17, No. 3 (Winter 1992/93): 84.

Boyd, John R. "A Discourse on Winning and Losing," briefing slides, Air University Library, Maxwell AFB, AL, August 1987.

Builder, Carl H. *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force.* New Brunswick, N.J.: Transaction Publishers, 1994.

Cable, Larry. "The Operation Was a Success, but the Patient Died: The Air War in Vietnam, 1964-1969," from *An American Dilemma: Vietnam, 1964-1973*, by Dennis E. Showalter & John G. Albert, 1993, 128, as reprinted in *Air War College Department of Strategy, Doctrine and Air Power Readings*, Vol. 2, Academic Year 1996. Maxwell AFB, AL: Air University Press, October 1995, 379.

Caro, Chuck de. "Sats, Lies, and Video-Rape: The Soft War Handbook," unpublished paper, Aerobureau Corporation, 1994.

Clausewitz, Carl von. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, NJ,: Princeton University Press, 1976.

Fadok, Major David S. *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis.* Maxwell AFB, AL: Air University Press, February 1995.

FM 100-20/AFP 3-20. *Military Operations in Low Intensity Conflict.* Washington, GPO, December 5, 1990.

Hallion, Richard P. *Storm over Iraq, Air Power and the Gulf War.* Washington: Smithsonian Institution Press, 1992.

JP 3-07, *Joint Doctrine for Military Operations Other Than War.* Washington, GPO, 16 June 1995.

Klingaman, Jerome W. "US Policy and Strategic Planning For Low-Intensity Conflict," from *Low-Intensity Conflict in the Third World*, compiled by Lewis B. Ware, et al. (Maxwell AFB, AL: Air University Press, August 1988), 164-165.

Mann, Col Edward C., III. *Thunder and Lightning, Desert Storm and the Airpower Debates.* Maxwell AFB, AL: Air University Press, April 1995.

Mason, Tony. *Air Power: A Centennial Appraisal*, Chapter 8, 1994, 238, as reprinted in *Air War College Department of Strategy, Doctrine and Air Power Readings*, Vol. 3, Academic Year 1996. Maxwell AFB, AL: Air University Press, November 1995, 15.

Metz, Steven and James Kievit. *The Revolution in Military Affairs and Conflict Short of War*. Carlisle Barracks, PA: Strategic Studies Institute, July 25, 1994.

Reynolds, Col Richard T. *Heart of the Storm, The Genesis of the Air Campaign Against Iraq*. Maxwell AFB, AL: Air University Press, April 1995.

Science Application International Corporation. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*. Joint Chiefs of Staff Report, 4 July 1995.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.

Smith, William D. "Weapons Proliferation, There Is No More Vital Research Than That Involving Defenses Against Theater Ballistic Missiles," in Vincent C. Thomas, Ed., *The Almanac of Sea Power 1996*, Vol. 39, no. 1, January 1996: 58.

Stein, George J. "Information Warfare," *Airpower Journal*. Spring 1995, 32.

Stein, George J. "Information War—Cyberwar—Netwar," Air War College Course 2104-B (Information Warfare) paper, Air University, Maxwell AFB, AL, Fall 1995.

Summers, Harry Jr. *On Strategy: A Critical Analysis of the Vietnam War*. Novato, Calif,: Presidio Press, 1982.

Szafranski, Richard. "Neocortical Warfare? The Acme of Skill," *Military Review*, November 1994, 47.

Toffler, Alvin and Heidi. *Creating a New Civilization, The Politics of the Third Wave*. Atlanta: Turner Publishing, Inc., 1995.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown, 1993.

Tzu, Sun. *The Art of War,* from *The Seven Military Classics of Ancient China*. Edited and translated by Ralph D. Sawyer and Mei-Chun Sawyer. Boulder, CO,: Westview Press, 1993. Also, *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971.

United States Department of the Air Force, Office of the Secretary of the Air Force. *Cornerstones of Information Warfare*. Washington, GPO, Fall 1995.

Watkins, Steven. "New Era has Humble Start," *Air Force Times*, November 20, 1995, 24.

Wood, Robert J. "*Information Engineering, The Foundation of Information Warfare*," Air War College Research Report, Air University, Maxwell AFB, AL, April 1995.

Young, Stephen. "How North Vietnam Won the War," *Wall Street Journal*, August 3, 1995, interview with Colonel Bui Tin, North Vietnamese army, as reprinted in the *Daedalus Flyer*, special reprint.